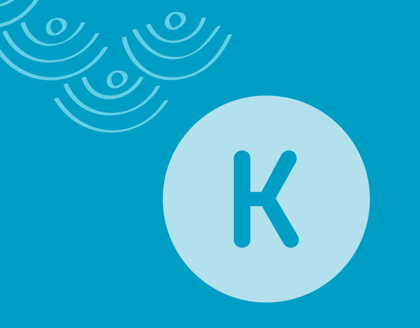
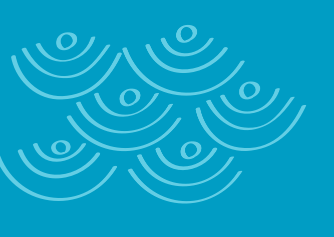




PRÁCTICAS QUE SALVAN

Guía de seguridad y privacidad digital para organizaciones de la sociedad civil colombianas.







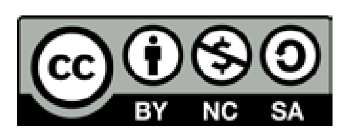
Fundación Karisma

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.

Más información sobre el tema en
http://www.documentoaccesible.com/#que-es.

Esta publicación fue realizada por la Fundación Karisma con el apoyo y financiación de Open Society Foundation.





Autora
Amalia Toledo

Revisión
Carolina Botero
Stephane Labarthe
Pilar Sáenz

Diseño editorial y gráfica
Roberto Guillén

Bogotá, Colombia
2019

TABLA DE CONTENIDOS

INTRODUCCIÓN

La seguridad digital incluye todas las normas, procedimientos, métodos y herramientas que nos ayudan a tener nuestra vida digital (la de una organización) mejor protegida de intrusiones no deseadas, de pérdidas o fugas de información, y de falta de disponibilidad de los servicios. No se trata de blindar toda red, sistema informático e información digital contra toda posible amenaza, sino de saber cuáles son nuestras debilidades y capacidades para poner en práctica medidas que nos ayuden a reducir los riesgos.

En tiempos donde se suele decir que la privacidad ha muerto, no está de más recordar que esta hace parte de nuestra batería de derechos humanos, por tanto, es necesario preservarla y cuidarla. Elevar nuestra seguridad y la de las organizaciones ayuda a mantener nuestra privacidad. Además, nos facilita ejercer otros derechos como la libertad de expresión, el acceso a la información o el derecho a asociación, entre otros.

Y es que hoy nuestras vidas y las de las organizaciones están mediadas por un sinnúmero de dispositivos digitales, de sistemas y redes informáticas, de herramientas tecnológicas, de cuentas, servicios y plataformas que nos facilitan el trabajo, pero también pueden suponer una amenaza. La seguridad digital existe para ayudarnos a comprender esas amenazas que enfrentamos en ese omnipresente universo digital para poder contrarrestarlas.

Esta guía, justamente, busca ofrecer algunas ideas a organizaciones de la sociedad civil colombiana para que mejoren su seguridad y privacidad digital, y, así, puedan fortalecer y proteger a su equipo humano y a las poblaciones con las que trabajan.

Esta guía es también el producto de varios meses de trabajo con un pequeño pero diverso grupo de organizaciones de derechos humanos, que nos abrieron sus puertas y confiaron en nuestro trabajo para evaluar el estado de su seguridad digital.

La muestra de organizaciones que hizo parte de este trabajo quizá no sea representativa de la multiplicidad de instituciones, grupos, redes y colectivos que trabajan en la defensa de derechos humanos en el país. No obstante, los resultados mostraron que hay ciertos temas comunes que toda organización puede considerar para promover una cultura institucional de seguridad y privacidad digital.

El trabajo que dio inicio a esta guía se realizó en varias fases, que incluyeron un diagnóstico previo de las prácticas digitales de las organizaciones, sus sistemas de información y arquitectura tecnológica; una sensibilización y formación básica al personal de las organizaciones, cuyo propósito no fue otro que inspirar la transformación a prácticas digitales más seguras; y una auditoría en seguridad digital *in situ* y a distancia para analizar a profundidad diferentes categorías (ej. seguridad física, organizacional, cuentas en línea, sitio web, etc.) y ofrecer una serie de recomendaciones, que se discutieron con el personal de la organización, para iniciar el camino de fortalecimiento de la seguridad y privacidad digital de las organizaciones.

La guía no pretende ser la norma por la que deberían guiarse las organizaciones de derechos humanos en Colombia en relación con la seguridad digital. Tampoco ofrece soluciones únicas e infalibles. Haríamos mal si creyéramos que eso es posible. Más bien, busca despertar el interés de las organizaciones por el tema, ofreciendo algunos consejos y vías a explorar, que deben considerar las capacidades, recursos, disposición y el nivel de compromiso de la organización para tener éxito.

Sería prudente tener en consideración algunas advertencias:

- No hay seguridad al 100%, siempre existirán riesgos y los dispositivos, sistemas y redes nunca estarán completamente asegurados.
- No hay una única solución para mantener la información o las comunicaciones seguras.
- Tampoco hay una única herramienta que proteja la información de toda amenaza.
- En la seguridad digital, la cadena es tan fuerte como el eslabón más débil, que normalmente somos las personas y nuestros hábitos.

Frente a esto, podemos afirmar que uno de los grandes desafíos de la seguridad digital es que es difícil implementarla. Y la mejor manera de garantizarla en una organización es cambiando el comportamiento humano. Esto requiere de la participación y compromiso de todo el personal de la organización, desde la dirección hasta los mandos más bajos. Si esta intención la acompañamos con un mejor uso de herramientas, servicios, tácticas y tecnologías digitales, estaremos en el camino adecuado para tener redes y sistemas de información más seguros y confiables.

Para tener organizaciones más seguras, tenemos que hacer un análisis de riesgo, que nos permita saber cuáles son las principales vulnerabilidades ante nuestra información y comunicaciones, y cuáles son las amenazas que podrían utilizar las vulnerabilidades. En la medida en que las organizaciones tengan clara esta identificación de riesgos, podrán establecer las medidas preventivas y correctivas que mejor se ajusten a sus capacidades y recursos para garantizar mayores niveles de seguridad digital.

De esta forma, en la guía ofrecemos recomendaciones que no representan ni mucho menos una lista cerrada de cosas por hacer, sino sugerencias de ideas a evaluar y decidir si son necesarias, si existe la capacidad en ese momento para implementarlas, si tienen los recursos, y si cuentan con el compromiso y la disponibilidad necesaria para desarrollar los cambios con éxito.

En las páginas siguientes, presentamos diferentes categorías de medidas de seguridad que, aunque es necesario que se crucen, permiten trabajar de forma compartimentada, con el fin de evitar la fatiga que suele provocar la seguridad digital. Cada sección inicia con un definición de la categoría, en la que buscamos establecer el marco de trabajo de cada parte.

En recuadros celestes, intentamos incluir información adicional que complementa algunas de las recomendaciones;

mientras que los recuadros amarillos ofrecen definiciones de conceptos que mencionamos para dar mayor claridad a las recomendaciones.

También hemos incluido dos secciones especiales sobre dos temas –el uso de WhatsApp y el problema de los trolles–, que resultaron recurrentes en el trabajo con las organizaciones de derechos humanos que nos permitieron desarrollar esta guía.

Finalmente, queremos agradecer la disposición y confianza depositada por todos los equipos humanos de las organizaciones con las que trabajamos, que preferimos no mencionar por razones de confidencialidad. Sin ellas esta guía sería imposible. Esperamos que lo que aquí proponemos sea de utilidad para iniciar un camino necesario, aunque arduo, para promover culturas institucionales más seguras y respetuosas de la seguridad y la privacidad digital.

CATEGORÍAS DE SEGURIDAD



SEGURIDAD ORGANIZACIONAL

La seguridad organizacional se refiere a aquellos aspectos relacionados con las políticas y procedimientos internos de una institución en relación con la seguridad de los sistemas y la información digital.

Este componente de la seguridad de las organizaciones, visto desde el lente de lo digital, suele dejarse en el olvido. Sin embargo, con unas simples acciones cualquier organización puede transformar sus prácticas institucionales en cuanto al manejo y tratamiento de los sistemas y la información digital. Es probable que ya tengan un camino recorrido en el ámbito de la seguridad física y que el paso a lo digital no sea complicado.

RECOMENDACIONES:

Política institucional de seguridad digital y persona encargada de hacer seguimiento a su implementación.

Esta política no tiene que ser compleja. Lo importante es que establezca normas básicas que sirvan de guía sobre las reglas y comportamientos esperados de todas aquellas personas en la organización que tienen acceso a los sistemas de información, redes, dispositivos y gestionan datos e información digital institucionales. Algunos aspectos que deberían estar cubiertos son:

- Creación y uso de contraseñas seguras.
- Uso de equipos que pertenezcan a la organización.
- Uso de cuentas de correo y redes sociales institucionales.
- Uso adecuado de servicios en la nube.
- Normas sobre copias de seguridad de la información (frecuencia, lugar de almacenamiento, etc.)
- Identificación de la(s) persona(s) encargada(s) para hacer seguimiento a la implementación de la política.
- Normas de seguridad digital en viajes de campo.

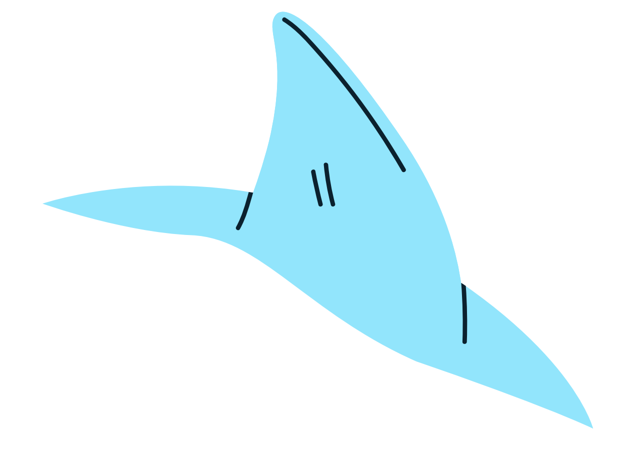
Tener un equipo humano sensibilizado y comprometido con la seguridad y privacidad digital.

Lo más difícil de la seguridad digital es cambiar hábitos y prácticas. Una forma de empezar esa transformación es a través de procesos de sensibilización y capacitación del equipo humano de la organización. Es importante que en este proceso se genere conciencia colectiva. Además, es primordial que haya suficiente implicación de todas las personas del equipo, incluida la dirección, cuyo papel es esencial para dar ejemplo y tomar decisiones relacionadas.

Para mejorar la seguridad digital de la organización es imperativo que quienes hacen parte del equipo humano entiendan por qué y cómo actuar.

Incluir una cláusula de confidencialidad y seguridad digital en los contratos de trabajo y acuerdos de pasantía y/o voluntariados.

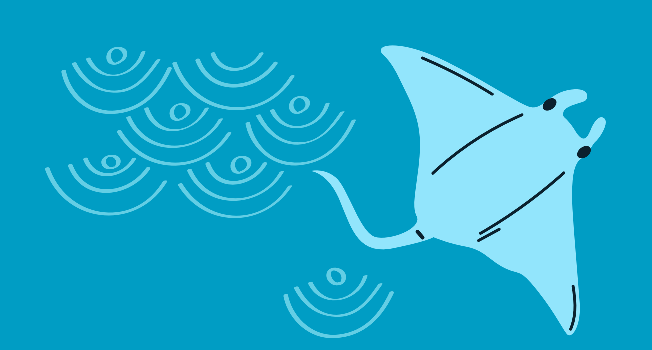
Está cláusula deberá establecer el parámetro entre la nueva relación de trabajo o colaboración en el que, de entrada, exista un compromiso para con la seguridad y privacidad digital de las personas y la información institucional a la que se tendrá acceso y se gestionará.





SEGURIDAD FÍSICA

La seguridad física se evalúa en torno a tres componentes: protección, detección e intervención. Sobre la **protección**, nos referimos a todos los elementos físicos que ofrecen defensa frente a posibles intromisiones: rejas, puertas de seguridad, cerraduras en los muebles con información o equipos importantes, etc. La **detección** es toda aquella medida que nos avisa sobre una posible intrusión: alarmas, sensores de movimiento, sistemas de video vigilancia, etc. Finalmente, **la intervención** se refiere a los planes de acción ante un caso de intrusión: celador, aviso automático a la dirección, etc.



La seguridad física requiere la protección de todos los elementos físicos y digitales en donde se almacenan datos e información. Esto quiere decir que hay que asegurar los inmuebles en donde se ubica la organización, todos los muebles o equipos que den acceso a información en físico o digital, y a las redes de la organización: archivadores, cámaras de video vigilancia, sensores de movimiento, routers, servidores, computadores, discos duros externos, teléfonos móviles, memorias USB, etc.

Lo importante es evaluar cuán protegidos están estos elementos y tomar medidas para reducir riesgos de intrusión no autorizada, robo o pérdida de información o de equipos, etc.

RECOMENDACIONES:

- Asegurar la entrada física de la oficina, así como otras vías de entrada menos usuales (ej. ventanas, puertas traseras), ya sea con puertas de seguridad, buenas cerraduras, rejas o cualquier otro elemento de seguridad.

- Identificar qué espacios de la oficina deben cerrarse con llave al finalizar la jornada laboral (ej. oficina de administración y dirección).

- Asegurar que los documentos sensibles y soportes de información digital (ej. memorias USB, discos duros externos, tarjetas de memoria de cámaras) estén guardados en armarios o espacios bajo llave.

- Destruir documentos sensibles de forma segura (ej. usar trituradora de papel).

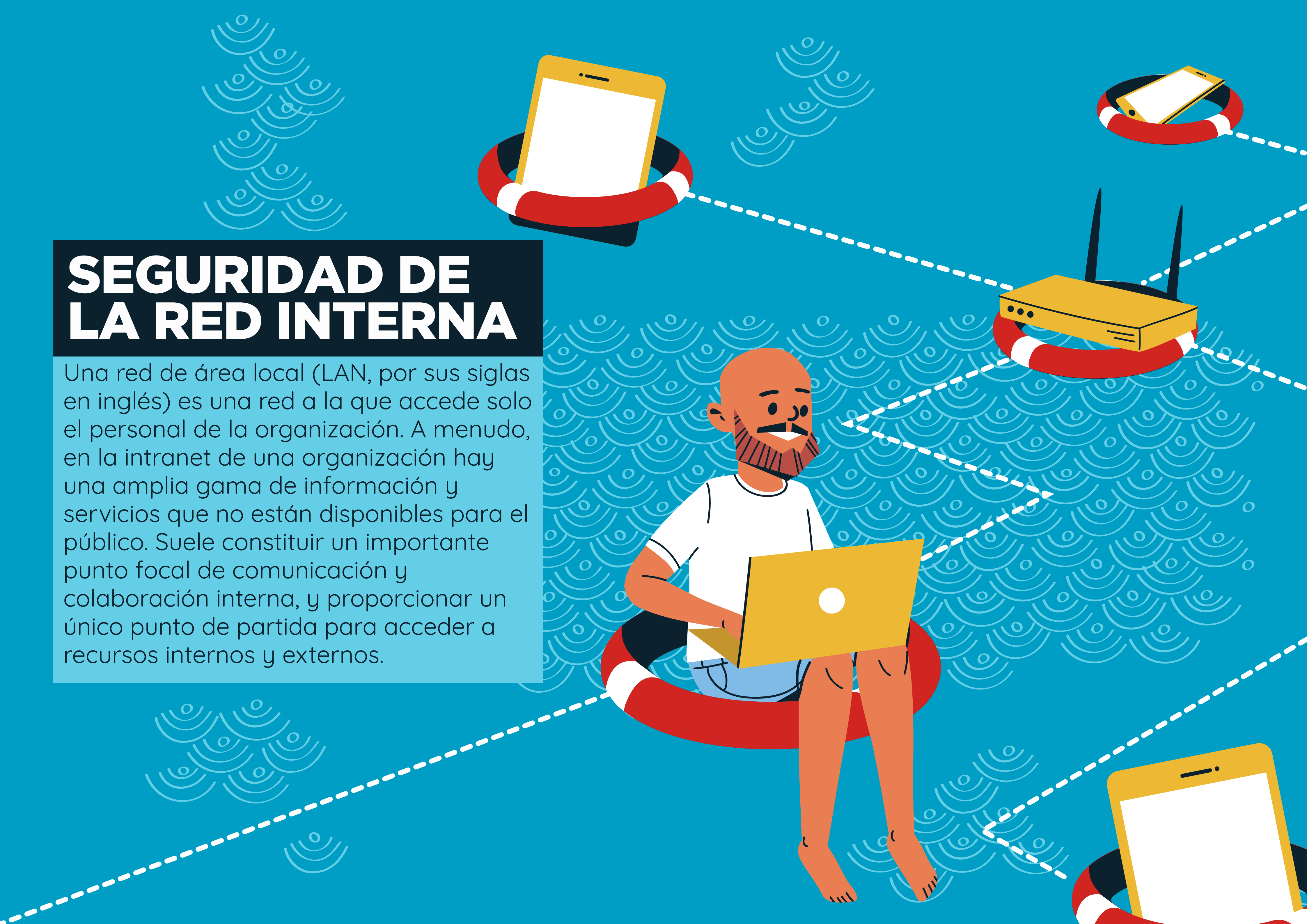
- Velar por el buen funcionamiento de los sistemas de detección e intervención, y hacer seguimiento de los contratos asociados.

- Si hay sistema de videovigilancia, colocar aviso de información sobre su uso.

- Si opta por instalar un sistema de detección e intervención, evalúe el uso de herramientas menos intrusivas que las cámaras de videovigilancia como los sensores de movimientos conectados a una alarma.

La recopilación de imágenes de personas implica el manejo de datos personales, de acuerdo con el Régimen General de Protección de Datos en Colombia. Por tanto, la implementación de sistemas de videovigilancia obliga a utilizar señales o avisos distintivos en las zonas monitoreadas.

Para más información, les recomendamos revisar la **guía orientativa** sobre protección de datos personales en sistemas de videovigilancia, elaborado por la Superintendencia de Industria y Comercio.



SEGURIDAD DE LA RED INTERNA

Una red de área local (LAN, por sus siglas en inglés) es una red a la que accede solo el personal de la organización. A menudo, en la intranet de una organización hay una amplia gama de información y servicios que no están disponibles para el público. Suele constituir un importante punto focal de comunicación y colaboración interna, y proporcionar un único punto de partida para acceder a recursos internos y externos.

Muchas organizaciones tienen una red local que les permite gestionar información y comunicaciones al interior de la organización, además de conectarse a internet. Algunas de esas redes están bien protegidas; otras prefieren compartir su acceso de internet con cualquier alma que se encuentre cerca.

Si bien puede ser un propósito loable abrir la conexión WIFI para que cualquier persona pueda navegar, la verdad es que esta práctica no es muy diferente a dejar nuestra casa abierta para que cualquiera entre, husmee, indague y se lleve lo que le plazca. ¡¿Quién hace eso?! Por el riesgo que implica, hay que prestar atención a la seguridad de esa red de área local.

La red de área local de una organización puede estar compuesta de servidores locales que prestan servicios como el de correo electrónico propios, de almacenamiento compartidos, de copias de resguardo automatizadas, etc.; además de cualquier dispositivos que se conecte a esa red.

RECOMENDACIONES:

- Si existe una red de conexión cableada, deshabilitar aquellos puntos que no estén en uso.
- Para las conexiones WIFI, usar el protocolo seguro WPA2 y contraseñas robustas.
- Si hay impresoras con capacidad para conexión inalámbrica, configurarlas para habilitar el protocolo WPA2 o desactivar su conexión WIFI para usarlas solo con cable.
- Si se usan carpetas compartidas en la red interna, configurarlas para que cada persona solo acceda a la información pertinente a sus labores e impedir el acceso por terceros no autorizados y accesos remotos.
- Para los *routers* que dan acceso a internet, cambiar la clave de administración del proveedor con una contraseña robusta y configurar las reglas del *firewall* de forma según necesidades identificadas.
- Para la red WIFI, si es posible, es mejor crear un acceso para invitados, distinto al que se conecta el personal de la organización. Esta red también debe usar el protocolo WPA2 y contar con una contraseña robusta.

El ***router*** es ese pequeño dispositivo que suele entregarnos nuestro operador de telecomunicaciones y que une varios equipos o redes informáticas a través de conexiones alámbricas o inalámbricas. Son los equipos que nos dan acceso a internet. Cumplen un papel importantísimo en la seguridad de la red, pues son la barrera de protección inicial entre la red interna e internet.

El **WPA2** se refieren a uno de los protocolos de cifrado inalámbrico que pueden utilizar los *routers* y nuestros equipos. Este protocolo tiene por objeto proteger la información que se envía y recibe a través de la red WIFI.

Un **cortafuego o *firewall*** es lo más parecido a un policía de tráfico digital que vigila los límites de la red. Se puede utilizar para evitar que cierto tipo de tráfico entre y/o salga de las áreas de la red; es una poderosa herramienta para la defensa contra ciberdelincuentes. Los *routers* pueden incorporar *firewalls*. Es recomendable revisar que estén activados y configurados de forma adecuada.




SEGURIDAD EN LOS DISPOSITIVOS

Para los efectos de esta guía, los dispositivos a los que nos referiremos en esta sección son los computadores de escritorio, los portátiles, las tabletas y los teléfonos inteligentes que utiliza el equipo humano de la organización. También incluimos soportes externos como memorias USB, discos duros externos y tarjetas de memorias de cámaras.




Este punto, en sí mismo, es de difícil implementación. Algunas organizaciones proveen de todos los dispositivos necesarios a su personal; otras solo tienen la capacidad de prestar equipos de escritorio a parte de ellos, mientras comparten algunos portátiles entre varios para los viajes de campo. Cuando hablamos de teléfonos inteligentes, es mucho más común que sean los dispositivos propios de las personas que trabajan en las organizaciones. A veces, incluso, estamos ante equipos humanos que, por razón de políticas internas, recursos y/o capacidades institucionales, utilizan sus propios computadores y otros dispositivos de forma cotidiana para labores de la organización. Esta diversidad de alternativas dificulta la gestión de la seguridad de los dispositivos utilizados en las labores de las organizaciones. No obstante, pueden establecerse políticas y prácticas básicas para cada circunstancia que ayuden a una gestión segura de estos dispositivos, que se utilizan en comunicaciones institucionales y contienen mucha información sobre la organización.

RECOMENDACIONES:

- Mantener actualizados los sistemas operativos y programas usados. En caso de usar el sistema operativo Windows, es importante tener licencias oficiales.

> Las actualizaciones de los sistemas operativos y programas informáticos usualmente incluyen parches de seguridad. Si no se actualiza, los agujeros de seguridad no "reparados" dejan nuestros equipos expuestos a ataques.

- Eliminar los programas informáticos que no se utilizan.
- Contar con un antivirus debidamente actualizado.
- Definir e implementar reglas mínimas para la configuración de seguridad y privacidad de los computadores.
- Definir e implementar quienes tendrán privilegios de administración en los computadores de la organización y crear cuentas de usuario para el resto de las personas que hacen parte del equipo humano de la organización.

> El **cifrado** es un procedimiento que permite transformar un mensaje, sin atender a su estructura lingüística o significado, en un código incomprensible o, difícil de comprender a toda persona que no tenga la clave secreta de descifrado. Cifrar los contenidos en un dispositivo es otra defensa contra intrusiones no autorizadas, pues sirve de barrera para acceder a la información. El cifrado puede realizarse sobre todo un disco duro, un soporte externo, un archivo o una carpeta. Muchos dispositivos tienen una función en sus sistemas operativos que permite cifrar el disco duro (ej. en iOS es **FileVault**; en Microsoft es **BitLocker**; en Linux, varía según la distribución que se instale). También hay programas como **VeraCrypt**, que permiten cifrar todo o parte de un volumen o carpetas, y **7-Zip** que cifra carpetas.

- Configurar claves de acceso únicas y robustas para cada usuario y en cada dispositivo.
- Cifrar el contenido de todos los computadores o, al menos, los archivos que contengan información sensible.
- Cifrar los datos sensibles que viajan en soportes externos como memorias USB o discos duros. Si cifrar no es posible, puede configurarse una clave de acceso robusta a los archivos con datos sensibles.
- Eliminar archivos de todos los dispositivos, incluidos los soportes externos y en particular los equipos que van a ser reemplazados o descartados, usando programas de borrado seguro.
- Definir e implementar una política de copias de seguridad en función de la importancia de la información de la organización, que incluya la periodicidad con la que se harán y el soporte dónde se almacenará, la(s) persona(s) responsables de hacer las copias y las medidas de seguridad para proteger estos dispositivos (ej. cifrado del contenido).

En el caso de los **teléfonos inteligentes,** encontramos mayor dificultad a la hora de implementar buenas prácticas de seguridad digital, sobre todo, porque suelen ser dispositivos omnipresentes, que usamos casi para todo, que almacenan muchísima información institucional y que suelen ser personales –no proporcionados por la organización–. A pesar de esto, podemos establecer unas reglas básicas de buen uso:

- Tener actualizado el sistema operativo de los teléfonos, si el dispositivo lo permite.
- Configurar el bloqueo automático del teléfono con contraseña o patrón de seguridad.
- Cifrar el contenido del teléfono, si lo permite.
- Cuidar las aplicaciones que se instalen y las autorizaciones que otorgamos.
- Eliminar las aplicaciones que no se utilicen.
- Eliminar la información innecesaria contenida en el celular (ej. contactos innecesarios, fotografías y mensajes irrelevantes).
- Hacer copia de seguridad de los datos importantes que contiene el celular (contactos, archivos, etc.).

Los métodos de borrado seguro de datos no son lo mismo que enviar archivos a la papelera de reciclaje del computador y eliminarlos. El primero “destruirá” de forma “permanente” los archivos, mientras que el segundo, aunque eliminará los datos, permite que sean fácilmente recuperables.

En iOS, el borrado seguro ocurre al dar clic a “Vaciar papelera”. En Windows, hace falta instalar un programa especializado como **Eraser** o **Blancco**. Para Linux, está disponible **BleachBit**. También existen programas similares para eliminar permanentemente archivos en móviles.




¿QUÉ HACER
CON WHATSAPP?

WhatsApp es increíblemente popular, tiene un cifrado de extremo a extremo (sistema de comunicación en el que solo las personas que se comunican pueden leer los mensajes) y, en ocasiones, es incluso gratuito o muy barato. Sin embargo, le falta algunas funciones de seguridad importantes, por lo que es mejor hacer un uso correcto de la aplicación.

Tenga en cuenta que los consejos que daremos a continuación recaerán únicamente sobre el contenido de los mensajes. Cuando se trata de los metadatos, los datos alrededor de la comunicación, es poco lo que podemos hacer. Y es que, aunque los metadatos no tengan nada que ver con lo que decimos, son datos que pueden decir mucho sobre quiénes somos, nuestras amistades y comunidad, a dónde vamos y cuándo utilizamos la aplicación. WhatsApp, a petición de una autoridad facultada para ello, podría entregar nombre, fecha de inicio del servicio, fecha de la última visita, dirección IP, dirección de correo electrónico, números bloqueados, información disponible en "Sobre", fotos de perfil, información de grupos y contactos, y hasta datos de localización.

En relación con el contenido que va por WhatsApp, si bien no es la opción más segura, podemos reducir algunos riesgos con los siguientes consejos:

1. Eliminar regularmente los mensajes o archivos que hayamos enviado/recibido, e incluso guardar la información de contacto bajo un nombre en clave. Esto es parte de la seguridad que tenemos que considerar en nuestras comunicaciones, sobre todo, cuando tenemos conversaciones con personas especialmente vulnerables. Tenga en cuenta que el cifrado de extremo a extremo con el que cuenta WhatsApp no evita que alguien con acceso al contenido de nuestro teléfono pueda leer los mensajes de WhatsApp.

2. Tener acuerdos de seguridad en los grupos. Para ello, podemos establecer claramente el propósito por el que se crea el grupo, los compromisos sobre el proceso para agregar nuevos miembros, la regularidad con la que se espera que se eliminen los contenidos, asuntos que podrán o no discutirse en el grupo, etc. Por ejemplo:

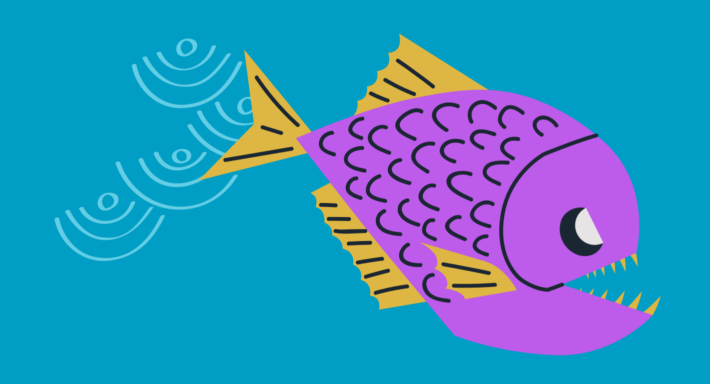
   Les damos la bienvenida al grupo [razón por la que se crea el grupo]. Por favor, no agregue nuevos miembros sin antes obtener la aprobación de al menos otros tres miembros. Por favor, borre los mensajes y otros archivos (ej. imágenes, videos, etc.) de este grupo de chat después de 3 días. Desactive la función de copias de seguridad en la nube para sus mensajes de WhatsApp. Por favor, no hable de las ubicaciones físicas en este grupo. Seguridad es solidaridad. ¡Gracias por su comprensión!

3. No asociar nuestro número de teléfono con Facebook y evitar tener esta aplicación en el teléfono. WhatsApp pertenece a Facebook, lo que significa que, si estamos en un grupo de WhatsApp, los contactos aparecerán como sugerencia en la red social. Desafortunadamente, si ya lo hemos hecho, la única opción que tendríamos es utilizar WhatsApp con un número diferente.

4. Realizar una copia de seguridad de cualquier contenido importante antes de eliminarlo. Sobre este tema, es importante considerar los riesgos de seguridad física que conlleva conservar o transportar los datos que hemos exportado o copiado localmente. Por eso, recomendamos cifrar los dispositivos.

5. No habilitar las copias de seguridad automáticas en iCloud o Google Drive. Aunque el contenido quedaría cifrado en los servidores de Apple y Google, estas compañías pueden estar obligadas por ley a entregar el contenido. En lugar de hacer una copia de seguridad en la nube, podemos hacer un registro de los chats y archivos que por razones de responsabilidad o conservación sea conveniente guardar. En ese caso, lo mejor es exportarlos y almacenarlos fuera de la app.

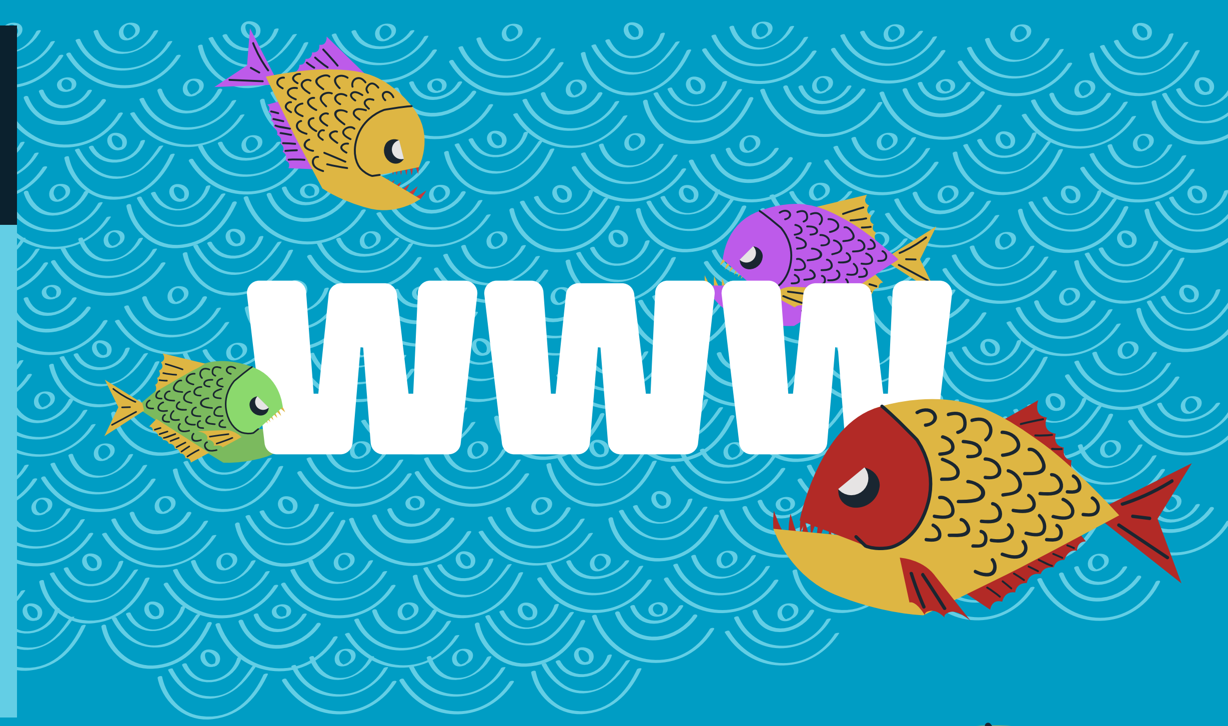
** Esta información está basada en el artículo **Harm Reduction for WhatsApp** por Dia Kayyali.*



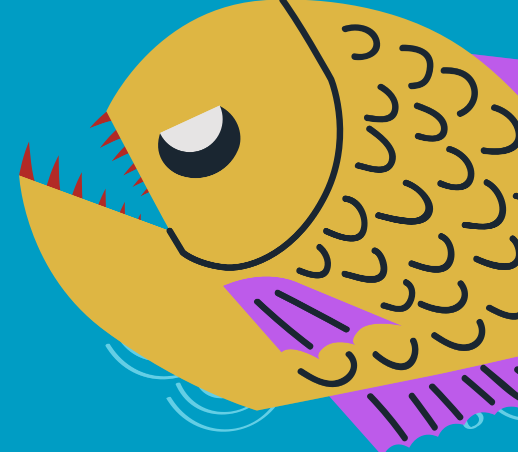


SEGURIDAD DE LOS SITIOS WEB

Es común que las organizaciones cuenten con uno o varios sitios web, es decir, un conjunto de páginas web con contenidos de muchos tipos (ej. multimedia, infográfico, imágenes, textos). El sitio web está identificado con un nombre de dominio y está alojado en un servidor web. Normalmente, el sitio web es administrado por una o más personas a través de un cuenta en un sistema de gestión de contenidos (ej. Wordpress o Drupal) y contraseña.







Los sitios web suelen cumplir una función elemental para las organizaciones de la sociedad civil. Son espacios virtuales que permiten dar a conocerlas; que sirven para almacenar y difundir diversidad de contenidos relacionados con el trabajo y misión de la organización; anunciar otros canales de comunicación (ej. redes sociales, correo electrónicos, números de teléfono), etc.

RECOMENDACIONES:

- Activar alertas de notificación para las fechas de vencimiento del nombre de dominio y del servicio de almacenamiento de la organización.
- Gestionar el dominio y sitio web desde una cuenta a nombre de la organización.
- Incluir información legal sobre protección de datos.
- Implementar el protocolo de transmisión segura de datos (HTTPS) en el sitio web y en la interfaz de administrador del sistema de gestión de contenidos (*content management system* o CMS).
- Mantener actualizado el servidor web donde está alojado el dominio, el sistema de gestión de contenido (ej. WordPress) y los complementos o *plugins* instalados en el sitio web.
- Al seleccionar el CMS, prestar atención no solo a la funcionalidad, sino también a la seguridad de las herramientas adicionales que se instalan en él (ej. *plugins*, plantillas).
- Reflexionar sobre la forma como usamos los datos de las personas que navegan el sitio para contemplar el uso de servicios de medida de audiencias (ej. Google Analytics) más amigables con la privacidad de las personas (ej. **Piwik/Matomo**, **Xiti**).

Los **dominios** son los nombres que utilizamos para identificar nuestro sitio web en internet. Si el nombre está disponible, podemos adquirirlo por un tiempo definido. Es necesario renovarlo cuando venza el plazo, de lo contrario, podemos perderlo.

El **alojamiento web** o ***web hosting*** es el lugar que ocupa un sitio web, correo electrónico, archivos, etc., en internet. Ese lugar es un servidor operado por compañías que, por lo general, hospedan varias aplicaciones o sitios web.

Un **complemento** o ***plugin*** es una aplicación que añade una funcionalidad adicional o una nueva característica al software, por ejemplo, incorporación de botones o mejora estética.

Un **certificado de seguridad (SSL/TLS)** sirve para brindar seguridad cuando se visita un sitio web. Es una manera de confirmar que el sitio es auténtico y confiable para ingresar datos personales. Si está habilitado, se pueden ver la siglas HTTPS y un candado cerrado en la barra de direcciones.






SEGURIDAD DE LAS CUENTAS EN LÍNEA

Al hablar de cuentas en línea, para efectos de esta guía, nos referimos a redes sociales, servicios de almacenamiento en la nube (ej. Google Drive, Microsoft OneDrive o Dropbox) y otros tipos para donaciones en línea, *crowdfunding*, etc.). La nube debe entenderse como los computadores de terceros, en este caso, de compañías de tecnología.




Las redes sociales son para las organizaciones de la sociedad civil ventanas a un enorme universo de posibilidades de interacción con sus audiencias. Tanto es así que algunas ni siquiera cuentan con sitios web propios, pues, su vida digital ha surgido a través de redes sociales. Ahí es donde se comunican e interactúan con el público, dan a conocer su trabajo, se organizan y establecen el tono con el que quieren ser conocidas.

Los servicios en la nube también facilitan el trabajo de las organizaciones, permitiendo el trabajo colaborativo y hasta la posibilidad de tener copias de los contenidos que generan. Además, son servicios que ayudan a reducir costos de infraestructura tecnológica y de mantenimiento.

Hay que reconocer que, en ambos casos, las empresas dueñas de estos servicios son las que hacen la inversión necesaria para mantener seguros estos servicios. Esto, sin lugar a dudas, es una ventaja para las organizaciones. Sin embargo, hay que tener en cuenta que estas empresas están legalmente obligadas a entregar datos a solicitud de una autoridad facultada para ello.

La información que recogen, además, pueden usarla para fines publicitarios o entregarla a socios comerciales y puede que esto no sea lo que queramos que hagan con nuestros datos.

Si vamos a usar redes sociales y entendemos que hay riesgos, podemos hacer una gestión más segura y consciente de las mismas siguiendo algunos consejos.



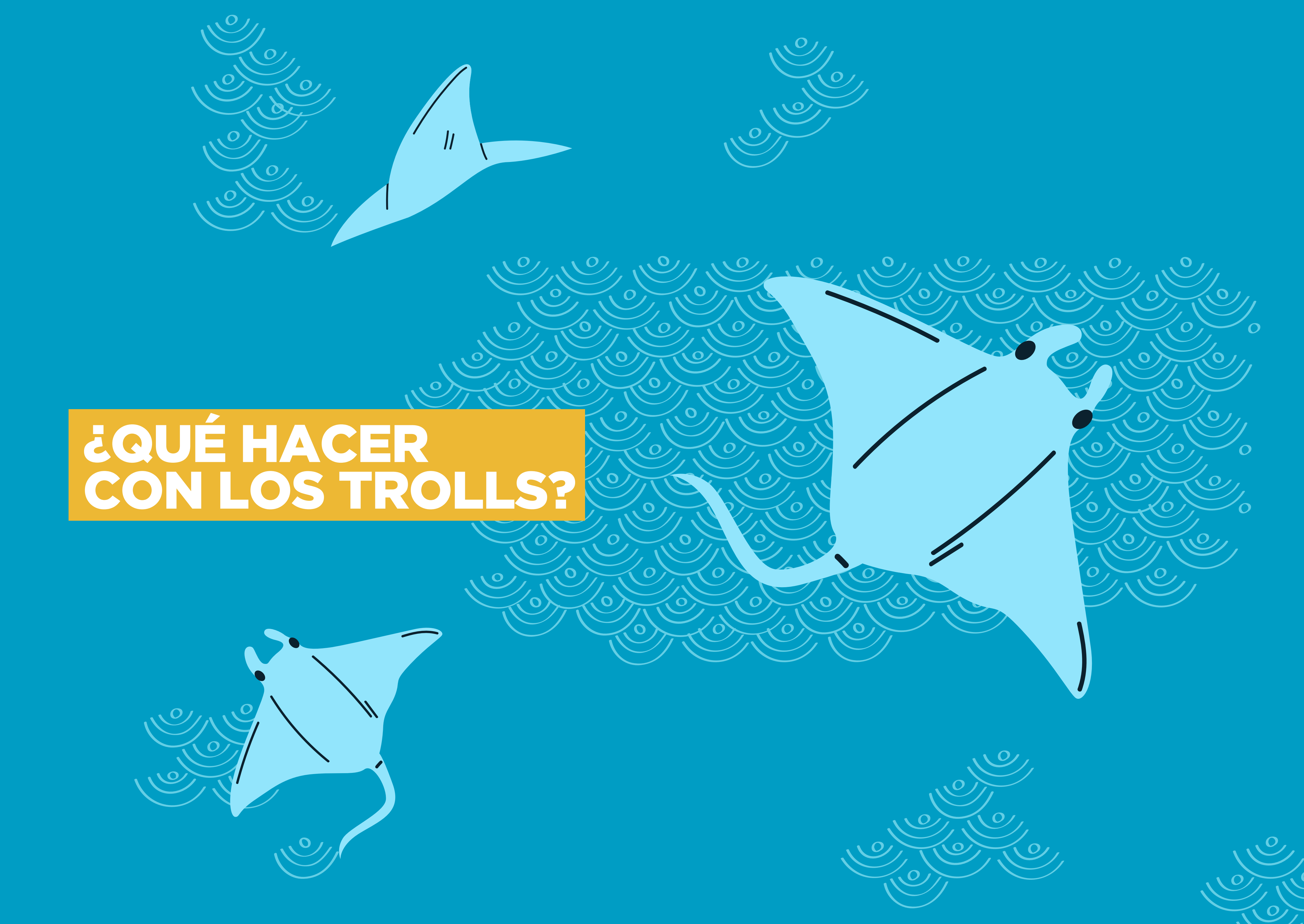
RECOMENDACIONES:

- Definir e implementar procedimientos para la gestión segura de cuentas de redes sociales y contraseñas en servicios en la nube (ej. cambiar contraseñas cuando hay rotación de personal encargado; manejar diferentes perfiles con diferentes niveles de acceso; tener copia de resguardo de usuarios y contraseñas).

- Utilizar correos institucionales para estos servicios, incluso para los correos de recuperación de cuentas.

- Pensar en buscar soluciones distintas a los servicios masivos de empresas como Google o Microsoft en función de los riesgos y el contexto de la organización. Algunas alternativas pueden ser soluciones de almacenamiento en un servidor de red local o servicios en la nube con políticas de privacidad robustas.

- Implementar el cifrado de los archivos con datos o información sensible, en caso de que sea necesario usar servicios en la nube como Google o Microsoft.



¿QUÉ HACER CON LOS TROLLS?

Vivir sin redes sociales es casi imposible y hoy contamos con vasta experiencia en cómo usarlas. La usamos para publicar artículos interesantes y relevantes, construir comunidad... en fin, para dar a conocer el trabajo de nuestra organización e interactuar con nuestra comunidad. Enfrentar trolls es también un ritual habitual. No importa lo que publiquemos, siempre aparecerá quien discuta o convierta nuestros comentarios en algo que parece imperdonable y erróneo. Y no importa lo que hagamos, parece imposible contenerlos.

Los trolls son personas –a veces también pueden ser *bots* o aplicaciones que corren automáticamente determinadas acciones en internet– que se esfuerzan activamente en causar problemas en internet. En la mayoría de los casos, los trolls son anónimos, pero no es un norma inquebrantable. Su característica más singular, que comparten con la figura mitológica del troll, es que parecen estar siempre enojados y buscan perturbar a menudo sin razón aparente. Las organizaciones de derechos humanos suelen ser un objetivo apetecible, sobre todo, si se dedican a temas que pueden ser disruptivos para el *status quo.*

¿Qué podemos hacer para enfrentar a los trolls desde una organización? Para empezar, somos de la opinión que hay que tener claras cuáles son las políticas de uso de las plataformas en las que participa la organización. Estas políticas deberían incluir comportamientos aceptables, además de las actitudes y conductas que puedan ser rechazables o eliminadas en todas las plataformas en donde se desarrollen las actividades de la organización (sitio web, FanPage de Facebook, cuenta de Twitter, etc.). Ahora bien, no basta con tener políticas, es igualmente imprescindible hacerlas públicas y comunicarlas.

También es importante que desde la organización se promueva el debate de ideas y el disenso. Está claro que nuestras posturas no serán del agrado de todo el mundo, por lo que debemos estar abiertos a la crítica, incluso aquella que resulta enfática, fuerte y hasta incómoda. Muchas veces distinguir los mensajes críticos de los que provienen de un troll es complejo, lo que nos coloca en la difícil decisión de no saber qué hacer.

Es usual que los trolles ataquen más fuerte si son ignorados, pero se validan cuando obtienen una respuesta, por lo que no hay solución simple. Lo primordial es no enfrascarse en una discusión fútil y desgastante. Entonces, la mejor apuesta es responder desde la empatía, mostrando que hay preocupación por los sentimientos y por la opinión de la persona. Hay muchas formas de responder: usando el humor, ofreciendo datos, o disculpándose, si es el caso, pero nunca debemos amenazar ni agredir. A partir de ahí, podemos evaluar lo que ocurra y decidir que hacer (volver a responder, dejar morir, bloquear, denunciar o eliminar) de acuerdo al siguiente esquema:



RECURSOS

Access Now. (s.f.). *Línea de ayuda en seguridad digital.* Información en **https://bit.ly/2ERVrCv.**

Asociación para el Progreso de las Comunicaciones. (s.f.). *Kit digital de primeros auxilios para defensores/as de derechos humanos.* Disponible en **https://bit.ly/2u2nASg.**

Electronic Frontier Foundation. (s.f.). *SurveillanceSelf-Defense. Autoprotección digital contra la vigilancia: consejos, herramientas y guías para tener comunicaciones más seguras.* Disponible en **https://ssd.eff.org/es.**

Fundación Karisma. (2018). *Currículo para personas auditoras de seguridad digital.* Disponible en **https://bit.ly/2DCHUOx.**

Fundación Karisma. (s.f.). *Genios de internet.* Disponible en **https://bit.ly/2sEEaWi.**

Fundación Karisma. (2017). *Seguridad, protección y privacidad en Twitter. Una guía para personas sobrevivientes de acoso y abuso.* Disponible en **https://bit.ly/2lnb3U1.**

Tactical Tech Collective. (s.f.) *Security-in-a-Box. Herramientas y tácticas de seguridad digital.* Disponible en **https://securityinabox.org/es/.**

The Engine Room. (2018). *Lazos que unen. Seguridad organizacional para la sociedad civil.* Disponible en **https://bit.ly/2SYOLHx.**

Wingu. (2017). *Manual de seguridad digital para OSC.* Disponible en **https://bit.ly/2O1VIXK.**

Fundación
Karisma





10 Consejos de seguridad digital para líderes sociales

1

Protegemos nuestros celulares.
Nuestros celulares tienen clave o patrón de acceso. Además, hacemos copias de seguridad con regularidad.

Más seguro: Si nuestros celulares lo permiten, ciframos sus contenidos.

2

Nos aseguramos de no dejar información en los computadores de terceros.
Cuando nos conectarnos desde un café internet, un espacio público o el computador de otra persona, usamos siempre el modo de navegación incógnita y recordamos borrar los documentos descargados.

Más seguro: Preferimos usar Firefox.

3

Nos comunicamos con herramientas seguras y ni siquiera las chuzadas nos escuchan.
Preferimos usar aplicaciones de mensajería que cifran las comunicaciones (ej. WhatsApp), que hacer una llamada telefónica o enviar un SMS.

Más seguro: Usamos las aplicaciones Signal o Wire, que son aún más seguras, y también les pedimos a nuestros contactos que lo hagan.

4

Nuestra navegación en internet es segura.
Revisamos la configuración de seguridad del navegador para deshabilitar rastreo y *cookies* de terceros, y borrar el historial.
Además, mantenemos nuestro navegador actualizado.

Más seguro: Usamos una red virtual privada (VPN) o el navegador **TOR** cuando queremos proteger nuestra identidad digital.

5

Tenemos copias de respaldo de nuestra información digital.
Con regularidad respaldamos la información que tenemos en computadores, celulares y en la nube.

Más seguro: Mantenemos más de una copia de respaldo y/o ciframos las copias de respaldo.

6

Cuidamos lo que publicamos en internet.
Protegemos nuestra privacidad y la de otras personas en internet evitando publicar fotos, información personal (números de identificación, teléfonos, direcciones, etc.) y ubicación. Además, tenemos cuidado al momento de decidir si etiquetamos fotos y mensajes.

Más seguro: Establecemos con cuidado quienes pueden ver o no cada publicación.

7

Cuidamos nuestras contraseñas.
Creamos contraseñas complejas, largas y diferentes para cada cuenta. Las cambiamos de vez en cuando, sobre todo, cuando sospechamos que pueden estar comprometidas (ej. si las usamos en un café internet).

Más seguro: Usamos un gestor de contraseñas como **KeePass**.

8

Protegemos la información sensible.
Los archivos con información sensible los protegemos con contraseñas de acceso.

Más seguro: Ciframos nuestros archivos sensibles con programas especializados como **7-Zip** o **Veracrypt.**

9

Protegemos nuestras cuentas en Facebook y otras redes sociales.
Usamos contraseñas seguras en nuestras cuentas. Para el *fanpage* de Facebook asignamos los roles (administrador, editor, moderador, etc.) y permisos con cuidado.

Más seguro: Utilizamos la autenticación de dos pasos.

10

Tenemos una vida digital saludable y segura.
Nos cuidamos en internet y en el mundo físico. Actualizamos las versiones de los programas que usamos en todos nuestros dispositivos, y revisamos con regularidad sus configuraciones de seguridad y privacidad.

Más seguro: Limpiamos nuestros equipos eliminando programas, aplicaciones, archivos e información no necesarios.